MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

Artificial Intelligence Memo. No. 126.

MAC-M-345
March 1967.

A Quick, Fail-Safe Procedure for Determining whether the GCD of Two Polynomials is 1.

Joel Moses.

One of the most widely used routines in an algebraic manipulation system is a polynomial manipulation package[1,2,3]. The crucial operation in such routines is the extraction of the Greatest Common Divisor (GCD) of two polynomials. This operation is crucial because of its frequent use and because it is an expensive operation in regard to time and space.

Experiments by Collins[1] have shown that given two polynomials chosen at random, the GCD has a high probability of being 1. Taking into account this probability and the cost of obtaining a GCD (some GCDs of polynomials of degree 5 in two or three variables can take on the order of a minute on the 7094[1]), it appears that a quick method of determining whether the GCD is exactly 1 would be profitable. While no such complete method is known to exist, a fail-safe procedure has been found and is described here. A fail-safe procedure is characterized by the fact that when it comes to a decision (in this case that the GCD is 1), then the decision is correct. However, the conclusion (i.e. that the GCD is 1) may be true, and the procedure need not arrive at a decision regarding it. It is believed that the fail-safe procedure presented here (and its extension to the linear case) will arrive at a decision quite frequently when the GCD is actually 1.

We shall first consider the case of polynomials of only one variable. The extension to several variables will be made later.

Let $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, a_i integers, $n>0$

$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0$, b_i integers, $m>0$

Let the operation of taking the GCD of A,B (both for integers and polynomials) be represented by (A,B).

Let $(P(x), Q(x)) = d(x)$ and let

$P(x) = d(x)\, r(x)$, $Q(x) = d(x)\, s(x)$.

For any integer a, then

$(P(a), Q(a)) = d(a)\,(r(a), s(a))$

Note that $(r(a), s(a))$ need not be 1 although $(r(x), s(x))$ is 1 when the GCD operation is over polynomials. Note further that the absolute value of $d(a)$ is always less than or equal to the GCD of $P(a)$ and $Q(a)$.

The plan for the procedure is as follows: We would like to substitute a number, a, say, into both $P(x)$ and $Q(x)$ and get the GCD of the results. This integer a is so chosen that the leading term of $d(x)$ will dominate the rest of the polynomial. In fact, we would like the leading term of $d(x)$ to be at least twice as large as the rest of $d(x)$. Thus even if the rest of the terms of $d(x)$ are of opposite sign from the leading term, we will be able to guarantee that the absolute value of $d(a)$ is at least one-half the absolute value of its leading term. If $d(x)$ be of degree k, $(k>0)$, then $d(a)$ would be at least $\frac{1}{2}a^k$. If $(P(a), Q(a))$ is less than $\frac{1}{2}a^k$, then $d(x)$ cannot be of degree k. If $(P(a), Q(a)) \geq \frac{1}{2}a^k$, then we do not have a decision regarding k.

In order to find a suitable candidate for a, we will need some information about $d(x)$. Without extensive calculation, it appears that we do not know the degree of $d(x)$ and certainly not its coefficients. We could, however, find a bound on the zeros of $d(x)$ since such zeros are roots of both $P(x)$ and $Q(x)$.

If we let R be the minimum of R_p and R_q, where R_p and R_q are bounds for the roots of $P(x)$ and $Q(x)$ respectively, then we find the following theorem applicable.

Theorem Let $R(\geq 1)$ bound the absolute value of the roots of $d(x)$, where $d(x)$ is a polynomial of degree $k>0$. Then for $x>3kR$ the absolute value of the leading term of $d(x)$ will be greater than twice the absolute value of the remainder of $d(x)$.

(Note: Thus if we choose a>3kR, where k is the minimum of m and n, then we could decide that the GCD is a constant (i.e. d(x) is of degree 0) if (P(a), Q(a)) < $\frac{1}{2}$a. We could decide that the GCD is 1 if we previously had taken care of constant GCDs by dividing P(x) and Q(x) by the GCD of their coefficients.)

Proof

Given that the roots are bounded by R, the condition regarding the leading term is hardest to satisfy when the coefficients of the remainder of the polynomial are as large as possible and of equal sign. This occurs in the polynomial $(x+R)^k$. The condition regarding the leading term can now be stated as

$$x^k > 2((x+R)^k - x^k), \quad x>0, \; R>0$$

$$\frac{3}{2}x^k > (x+R)^k$$

$$(\frac{3}{2})^{\frac{1}{k}} \; x > x + R$$

$$x > \frac{1}{(\frac{3}{2})^{\frac{1}{k}} - 1} R$$

The following lemma will complete the proof.

Lemma $\dfrac{1}{(\frac{3}{2})^{\frac{1}{k}} - 1} < 3k$, k a positive integer

Let $S = \sum_{i=0}^{k-1} (\frac{3}{2})^{-\frac{1}{k}} \quad (\frac{3}{2})^{-\frac{i}{k}}$

By the formula for finite sums of geometric progressions

$$S = \frac{(\frac{3}{2})^{-\frac{1}{k}} \; (\frac{3}{2})^{-\frac{k}{k}} - (\frac{3}{2})^{-\frac{1}{k}}}{(\frac{3}{2})^{-\frac{1}{k}} - 1} = \frac{(\frac{3}{2})^{-\frac{1}{k}} \quad \frac{1}{3}}{1 - (\frac{3}{2})^{-\frac{1}{k}}}$$

Each term in S has value <1. There are exactly k terms in S. Hence S<k

$$S = \frac{(\frac{3}{2})^{-\frac{1}{k}} \quad \frac{1}{3}}{1 - (\frac{3}{2})^{-\frac{1}{k}}} < k$$

$$\frac{(\frac{3}{2})^{-\frac{1}{k}}}{1 - (\frac{3}{2})^{-\frac{1}{k}}} < 3k$$

$$\frac{1}{(\frac{3}{2})^{\frac{1}{k}} - 1} < 3k$$

We have yet to obtain a complete procedure since we lack a bound on the roots of P(x) and Q(x). A simple bound for the roots of P(x) is $n \max \left[\frac{a_i}{a_n} \quad 0 \leq i \leq n-1 \right]$

This is a crude bound since for $(x+R)^n$ it yields nR^n instead of R. Several other easily calculable bounds are known, but we shall leave this problem to numerical analysts.

Now let us sum up the procedure defined above. We find the minimum of the bound on the absolute value of the roots of P(x) and Q(x). Call it, R, say. We pick an integer, a, say, such that $a > 3kR$, where k is the minimum of the degrees of P(x) and Q(x). If we let $g = (P(a), Q(a))$ then if $g < \frac{a}{2}$ and if we previously ascertained that the coefficients of P(x) and Q(x) had no common GCD, then we can guarantee that $d(x) = (P(x),Q(x)) = 1$. Otherwise no decision is made.

Extensions to the Basic Procedure.

Linear GCD

Let $g = (P(a), Q(a))$ (where a is chosen by the procedure above). If $g < \frac{a}{2}$, we know $d(x) = 1$. Suppose, however, $\frac{a}{2} \leq g < \frac{a^2}{2}$ at worst d(x) could be linear in x, that is, $d(x) = cx + d$ $(c \neq 0)$. We propose now to extend the scheme defined above in order to determine whether d(x) is linear. If d(x) is linear then this extended procedure will find it; if it is not, then d(x) must be 1; and then we have extended the range of applicability of the procedure for determining whether the GCD is 1.

As it turns out we can attempt to find all possible linear GCD by an extensive search since there are restrictive conditions on c and d.

We know that

$$c \mid (a_n, b_m), \quad d \mid (a_c, b_o) \quad \text{where} \quad e \mid f$$

means that e divides f

We might be able to avoid testing some or all possible linear d(x) by making use of the fact that d(a) divides g. For any pair, c,d, such that ac + d does not divide g, we can conclude that cx + d is not a possible d(x). If ac + d does divide g, then we shall evaluate $P(-\frac{c}{d})$, $Q(-\frac{c}{d})$. Both of these numbers must be zero. If they are, d(x) = cx + d. If no possible pair of values for c and d works, then d(x) = 1.

Extension to Several Variables

One can extend the procedure for several variables merely by substituting small integers for all but one of the variable and determining whether the resulting polynomials have a GCD of 1. If they do the original polynomials did also; if they do not then no decision is made. This idea is due to M. Manove who programmed it in MATHLAB[3], and existed prior to our result. It is likely that Manove's idea by itself will yield a very large saving of effort since the computation of GCDs grows very badly when the number of variables is increased.

The procedure was attempted on the pair of quartics given in (1). The evaluation was attempted for values of a between 100 and 150. Most GCDs resulted in numbers less than ½a, thus yielding the conclusion of a GCD of 1. In the ten cases that did not, the linear case settled the matter quickly since ac + d, for possible values of c and d, did not divide the GCD with one exception at a = 109.

For larger pairs of polynomials (say, of degree 30) the evaluation will have to be attempted on relatively large numbers (on the order of 1000). Thus one would have to resort to variable precision arithmetic. We must consider, however, that the evaluation of the GCD of such polynomials by straight forward methods would also require variable precision integer arithmetic.

It is hard to estimate, at present, the effect on running time that the introduction of a fail-safe method will have on the calculation of a GCDs. A gain in speed of an order of magnitude or better is not out of the question. If the fail-safe technique gains acceptance, then research is likely to yield various methods with differing costs and ranges of applicability.

Evaluation.

The success of the method depends, in large measure, on the likelihood that the GCD of r(a) and s(a) will be fairly low. Below we give an encouraging result which shows that if r(a) and s(a) were chosen at random, using a flat distribution, then the probability that their GCD is greater than 1 is less than 0.4. The meaningfulness of this result in practical situations is hard to gauge at present. It does, however, give one great hope for the success of the method.

Theorem. Let b be any integer chosen at random from $1,2,\ldots,N$ The probability that an integer less than b is relatively prime to b approaches $\frac{6}{\pi^2}$ (~ 0.6)

as N approaches ∞

Proof: The number of integers less than b and relatively prime to it is

$b \prod (1 - \frac{1}{p})$, where $p|b$ and p is a prime

That number can be written as

$b \prod (1 - \frac{1}{p} \Pr(p|b))$, where $\Pr(p|b)$ is the probability that p divides b which is 1 if $p|b$ and 0 otherwise.

Now if we allow b to vary, $\Pr(p|b) = \frac{1}{p}$, that is, the probability that b is even is $\frac{1}{2}$, that b is divisible by 3 is $\frac{1}{3}$, etc.

Thus, the number of integers less than b and relatively prime to it becomes,

$$b \prod \left(1 - \frac{1}{p}\frac{1}{p}\right) = b \prod \left(1 - \frac{1}{p2}\right), \text{ where p is a prime.}$$

But,

$$\prod_{p,\ a\ prime} \left(1 - \frac{1}{p^s}\right) = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n^s}}$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Thus

$$b \prod \left(1 - \frac{1}{p^2}\right) = b \frac{6}{\pi 2}$$

(The theorem used above may be found in any book on the Riemann Zeta Function).

This estimate for the probability is already known. The proof above is due to W. Henneman.

We would really be interested in knowing the probability that (r(a), s(a)) < e, for small integer values of e. Certain theoretical considerations indicate that for e = 10, the probability is greater than 0.9. However, these considerations are based on certain assumptions regarding the distribution of numbers relatively prime to a given number. In experiments we performed these estimates were off by one to two per cent. Nonetheless all signs point to the fact that if r(a) and s(a) were chosen at random, a high value for their GCD is very unlikely.

Acknowledgements

I would like to acknowledge useful discussions with B. Bloom, C. Engelman, W. Henneman and W.A. Martin.

References

1. Collins, G.E. "PM, A System for Polynomial Manipulation," CACM, August 1966, 578-589.

2. Brown, W.S.,Hyde, J.P., Tague, B.A. "The ALPAK System for Non-Numerical Algebra on a Digital Computer - II," BSTJ, March 1964, 785-804.

3. Manove, M., Bloom, S., Engelman, C. "Rational Functions in MATHLAB," MITRE Corp. Report MTP-35, August 1966.